Volume 4, Issue 7, July 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A New Technique for Handwritten Offline Signature Authentication System

Neha Rajpal
Computer Science Department,(GJU),MITM, Jevra, Hisar, Haryana 125001, India

Bhanu Arora
Computer Science Department, (PTU),RIET, Phagwara, Punjab 144401, India

Abstract--Handwritten signature is widely used for authentication and identity of an individual. Now a days Signature verification is one of the most important feature for checking authenticity of a person .Many kind of security parameters like password, finger printing checking, pincode are there but signature recognition is most popular because of its cost effectiveness and its accuracy .Signature Recognition is generally non vision based. There are various approaches to signature recognition with a lot of scope of research .This paper consist of offline signature verification system based on the combination of preprocessing, feature extraction such as global feature, grid feature, area ratio, normalized area etc .In this genuine signatures are taken from different person .After that preprocessing and feature extraction work applied on the signatures. By using Eucledian distance acceptance range is set between reference signature and training signatures .if the queried signature is in acceptance range than it is authenticated else, it is forged. Than we calculate the FAR, FRR and CRR to check the system performance and accuracy.

Keywords: Signature Verification, Preprocessing, Feature Extraction, Euclidian Distance, FAR(False Acceptance Range) , FRR(False Rejection Rate) , CRR(Correct Classification Rate).

I. INTRODUCTION

Signature verification is a biometric verification which is an important research area targeted at automatic identity verification such as legal, banking and high security environments.[1] Signature verification can be divided into two classes online and offline .Online approach uses a stylus and electronic tablet. Stylus which is connected to a computer to extract information about a signature and dynamic information like pressure, speed of writing, velocity etc which is used for verification purpose. Offline signature verification involves less electronic control and uses signature images captured by scanner or camera. In this features are extracted from scanned signature image and these features are very much simple[2].Difficulty lies in the fact that it is hard to segment signature strokes due to highly stylish and unconventional writing styles and non- repetitive nature of variation of signature because of age ,illness and emotional state of a person.[3]when we couple all these it causes a large variation. A robust system has to be designed that should consider all these type of factors but also detect various type of forgery. System should neither be too coarse nor too sensitive. It should have acceptable trade–off between low False Acceptance Rate and a low False Rejection Rate.

A.Types of forgery

There are various types of signature forgeries, some of them are:

1)Random Forgery: In this signature is written by the person, who don't know the shape of original signature. It is very simple and can be uncovered easily. It can also be named as Hit or miss Forgery.

2)Simple Forgery: It is represented by a signature sample which written by the person who know the shape of original signature without much practice. It is also called Amateur Forgery.

3)Skilled Forgery: It is represented by suitable imitation of genuine signature mode.it is also called Well-Versed Forgery[4].

B. Issues in Offline Signature Verification

A lot of research work has been done in the field of signature verification and bunch of solutions has been introduced to overcome its limitations and to compensate for the loss of accuracy.
Mostly two type of problem come across the researchers.

- Dynamic information can lost.
- Low quantity of available signature versus high number of extracted features.

First problem is addressed by some researchers [7][8],but there is still a challenging problem. Luana batista have mentioned some remedies for second problem.

- Select the most discriminating features.
- Use regulation techniques to obtain a stable estimation of the covariance matrix.
- Generate synthetic samples.
- Use dissimilarity representation.[9]

II. STEPS INVOLVED IN SIGNATURE VERIFICATION

There are various steps which need to be followed for verification of handwritten offline signatures,which are explained below:

- Data Acquisition
- Preprocessing
- Feature Extraction
- Training and Testing

A. Data acquisition

Images are scanned using a digital scanner and these images are store digitally for image processing.

B. Preprocessing

Preprocessing of image is a necessary step to improve the accuracy of Feature Extraction and to reduce their computational needs. The purpose of preprocessing is to make signature standards and make it ready for feature extraction.
The steps involved in it are:-

1)Noise reduction: A noise filter (like median filter) is applied to remove noise caused during scanning.

2) Resizing: The image is cropped to the bounding rectangle of the signature.

3) Binarization: It involves the transformation from color to grayscale, and then to binary.

4)Thinning: Its goal is to eliminate the thickness differences of pen by making the image one pixel thick.its aim is to reduce the character features to help in feature extraction and classification.

5) Clutter Removal: If there are some black dots which are unconnected it will remove that dots before processing

6)Skeletonization: It is used to remove selected foreground pixels from the binary image.So,its outcome is the representation of a signature pattern by collecting all thin arcs and curves.it is performed on a Binary image after the size of a image is fixed.

C. Feature extraction

Feature Extraction is the key process to achieve high accuracy in signature verification. An ideal feature extraction technique uses minimal feature sets that is used to maximize interpersonal distance between signature samples of different individuals while minimizing intrapersonal distance for those belonging to the same individual[5].
Feature Extraction is divided into main two types:

- Local Feature
- Global Feature

Local Features are extracted from a portion or a limited area of the signature image. These features are applied to the cells of a grid virtually super imposed on a signature image or a particular elements obtained after signature segmentation. These features are calculated to describe topological characteristics of local segments such as position, tangent direction and curvatures.

Global Features categorize the signature as whole. These features are extracted from all the pixels that lie within the region circumscribing the signature image such as length, width or baseline of the signature [6].

The following global and geometric features are extracted from pre-processed signature image.

1)Actual Height: The height of the binary signature image after removal of vertical blank spaces is called its Actual height.

2)Actual Width: The width of the binary signature image after removal of horizontal blank spaces is called its Actual width.

3)Maximum horizontal and vertical histogram: Horizontal histogram is calculated by going through each row of the signature image and counting number of black pixels. A row with maximum number of black pixels is recorded as

maximum horizontal histogram. Similarly, a vertical histogram is calculated by going through each column of the signature image and finding a column with maximum number of black pixels.

4)Normalized Area of signature: It is the ratio of exact area of signature image to the area of signature enclosed in bounding box. Area of a signature is the number of pixels comprising it.

Normalized area=Signature Area/
Area enclosed in a bounding box

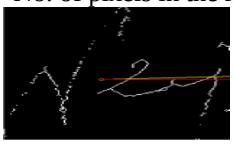
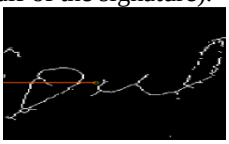
5)Aspect Ratio: It is defined as the ratio of actual width of the signature to the actual height of the binary signature. This is calculated because width or height of person's signature may vary but its ratio remains approximately equal.

Aspect Ratio=Actual width of signature in a bounding box/
Actual height of signature in a bounding box.

6)Centroid: The white pixels which belong to the binary signature image are treated as ON pixels. Centroid is the average coordinate point of all ON pixels of the binary signature image.

7)Ratio of Signature Occupancy of each half: Signature image is divided into two halves vertically. Then the ratio of number of pixels which belong to the left half of the signature image to number of pixels which belong to the right half of the signature image is calculated. It provides information about the signature occupancy ratio of two halves of the signature image.

Signature occupancy ratio= (No. of pixels in the left half of signature /
No. of pixels in the right half of the signature).

First half of the image. Second half of the image.
Fig.1. Showing First and Second half of Image.

8)Skew Angle: The first step is splitting the image into two equal parts. Then in each part of the image, the centroid is calculated. The angle between the horizontal axis and the line formed by joining the two centers of masses is calculated.

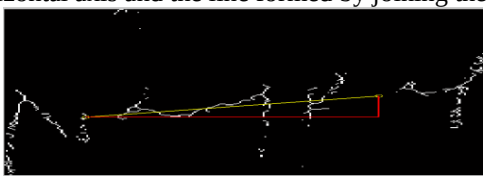


Fig.2. Skew Angle

9)Orientation of signature: It is the difference between the vertical centroids of the two equal halves of signature divided vertically. This indicates the overall orientation of the signature.

10)Ratio of distance between centroids: The Signature is divided vertically into 3 equal parts then centroid of each part is calculated. The distance between the centroid of first part and the centroid of middle part is calculated through x axis then the distance between centroid of middle part and centroid of third part is calculated . Atlast the ratio between them is calculated.

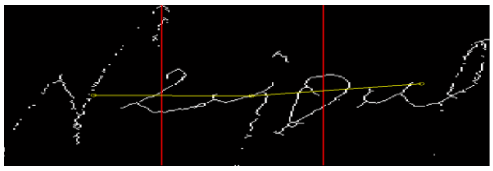


Fig.3. Ratio of distance between centroids

11)Ratio of Enclosed Area to the Bounding box area: After finding four equal parts as described above, the centroid of each part is calculated. After finding these centroids they are connected to each other. Then the area enclosed by these centroids connecting lines is calculated, in fig 10 it is shown by yellow triangle. Then the ratio between this area and the bounding box area is calculated. The size of the signature may vary but this ratio stay almost constant.

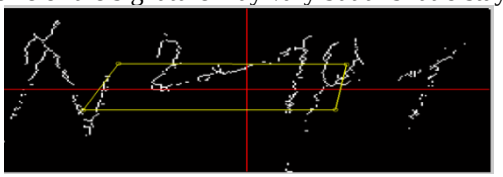


Fig.4. Ratio of Enclosed Area to the Bounding box area

After obtaining these global geometric features, we combine these features sets into a feature vector which is then fed to the trained system where the classifier uses it for generating matching scores and classify a signature as a genuine or forged.

D.Training and Testing

After the extraction of above described features from the collection of the sample signature images of different persons. The mean values and standard deviations of all the features are computed and used for the final verification.

Let μ_i and σ_i represents the mean value and standard deviation for the i^{th} feature and F_i denotes feature vector value for the query image. The Euclidian distance δ in the feature space measures the proximity of a query signature image to the mean signature of the claimed person.

$$\delta = (1/n) \sum_{i=1}^{n} [(F_i - \mu_i)/ \sigma_i]^2$$

The maximum and minimum Euclidian distance values of training signature samples are used to set the acceptance range. If the Euclidean distance of the query signature image with respect to mean signature image is within the acceptance range, the query signature is authenticated otherwise it is detected as a forged one.

III. METHODOLOGY

The procedure we are following to implement signature verification process is:

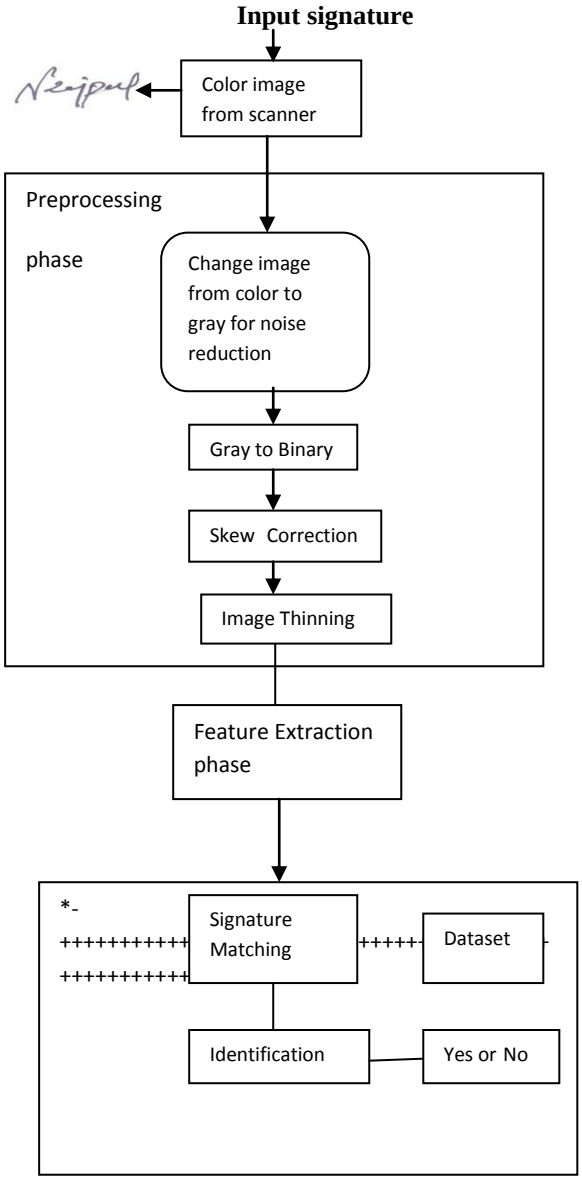


Fig.5. Procedure for Signature Verification

IV. RESULTS AND DISCUSSION

In this paper we have taken 46 genuine signatures and 60 forged signatures. Feature points are extracted by comparing 46 genuine signatures. For training and testing of system these signatures are used. These signatures are taken from 6 different persons. Different percentage values have been used to measure the performance of the system. We have calculated:

A.FAR
B.FRR
C.CCR
D.AER(Average Error Rate)
E.EER(Equal Error Rate)

1)FAR (False Acceptance Rate): The false acceptance ratio is given by the number of fake signatures accepted by the system with respect to the total number of comparisons made and is given by:

FAR = (No. of forgeries accepted *100)/
(No. of forgeries tested)

2)FRR (False Rejection Rate): The false rejection ratio is the total number of genuine signatures rejected by the system with respect to the total number of comparisons made and is given by:

FRR = (No. of genuine rejected *100)/
(No. of genuine tested)

3)CRR(Correct Classification Rate): It is the percentage of signatures those are exactly classified.

CRR= (No. of signatures correctly classified*100)/
(No. of genuine+ No. of forged signature)

*4)AER(Average Error Rate):*It is the average of FAR over FRR.

AER=FAR/FRR

*5)EER(Equal Error Rate):*It is the location on a ROC or Detection Error Trade off curve where the FAR and FRR are equal.Smaller the value of EER, better the system performance.[10]
The purpose of verification is to reduce FAR and FRR and increasing the accuracy.

V. TABLE

Table shows the result obtained on testing with datasets collected from different people.

Table1.Testing Results

Sample presented	**Genuine**	**Forged**	**FAR**	**FRR**	**CRR**
46 **genuine**	15	10	-	28.26%	86.79%
60 **forged**	-	45	10%	-	

VI. CONCLUSION AND FUTURE SCOPE

A human expert is able to identify skilled forgeries with an error rate of 1%. But when tested against skilled forgeries, even the best system is not able to deliver error rates less than 5% [11]. To overcome this, it is essential to identify, understand and compensate for the different sources of error in the algorithms. Cost of an error in signature verification is very high. An automatic signature verification system can come into existence only when its error rate is equal or below the human error rate (1%). User acceptance, level of security required, accuracy, Cost & Implementation these are the basic parameters that must be considered while designing a signature verification system [12].

A number of methods for Offline Signature Verification have been purposed. A new method to extract features from handwritten signature and verification of it is presented here. The proposed method promises a very simple but reliable solution to the problem of signature verification. A larger database can reduce false acceptances as well as false rejections. Using a higher dimensional feature space and incorporating dynamic information gathered during the time of signature can also improve the performance.

REFERENCES

[1] *Off-line Signature Verification* Mrs. Tulsi Gupta Student of M.Tech (Weekend Programme) IT, Guru Gobind Singh Indraprastha University, Dwarka.

[2] Offline *Signature Verification using Grid based and Centroid based Approach*(Sayantan Roy,Department of Computer Science Engineering),ISM Dhanbad Jharkhand.

[3] ISS(A u g 2 5 , 2 0 1 3)Offline Signature Verification System with Gaussian Mixture Models(GMM)Charu Jain1, Priti Singh2, Preeti Rana3.

[4] *Offline SignatureVerification Using Fusion of GeometricFeatures and Contour based features*.Sonika Gill,[M.Tech (CSE), RGGI Meerut],Beenu Yadav[M.Tech (CSE), RGGI Meerut].

[5] A.C. Verma, et al International Journal of Computer and Electronics Research [Volume 2, Issue 2, April 2013].1,2,3Department of Electronics & Communication Engineering, Sikkim Manipal Institute.

[6] *Offline Signature Verification System with Gaussian Mixture Models(GMM)* Charu Jain1, Priti Singh2, Preeti Rana31Research Scholar, Amity University Haryana. Department of Electronics and Communication, Amity University Haryana.

[7] Basavaraj L and Sudhaker Samuel R D. 2009. *Offline-line Signature Verification and Recognition - An Approach Based on Four Speed Stroke Angle*. International Journal of Recent Trends in Engineering, Vol 2, No. 3, November 2009.

[8] Zimmer A and Ling L L. 2003. *A Hybrid On/Off Line Handwritten Signature Verification System*. Proceedings of the Seventh International Conference on Document Analysis and Recognition (ICDAR 2003).

[9*]* *Approaches and Issues in Offline Signature Verification System*.HemantaSaikia(Depof Electronics & Communication Engineering Sikkim Manipal Institute of Technology Majitar, Sikkim, INDIA .Kanak Chandra Sarma(Department of Instrumentation & USIC Gauhati University, Guwahati, Assam, INDIA).

[10*]* *Approaches and Issues in Offline Signature Verification System*.Hemanta Saikia(Dept of Electronics & Communication Engineering Sikkim Manipal Institute of Technology Majitar, Sikkim, INDIA).Kanak Chandra Sarma(Department of Instrumentation & USIC Gauhati University, Guwahati, Assam, INDIA).

[11] Kovari B, Toth B, Charaf H. 2009. *Classification Approaches in Off-Line Handwritten Signature Verification*. WSEAS TRANSACTIONS on MATHEMATICS Issue 9, Volume 8, September 2009.

[12] Jain A K, Ross A and Prabhakar S. 2004. *An Introduction to Biometric Recognition*, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, January 2004.

